

Army Regulation 381-45

Military Intelligence

Investigative Records Repository

**Headquarters
Department of the Army
Washington, DC
25 August 1989**

SUMMARY of CHANGE

AR 381-45

Investigative Records Repository

This revision--

- o Redefines the responsibilities of the Deputy Chief of Staff for Intelligence; the Commander, U.S. Army Intelligence and Security Command; and the Commander, U.S. Army Central Security Facility in relation to the Investigative Records Repository (RR) (para 1-4).
- o Defines the categories of files authorized for IRR retention (para 2-1).
- o Establishes procedures for processing information protected by the Privacy Act (paras 2-1, 2-2, 2-3, and 2-6).
- o Modifies qualifications for file procurement officers (para 3-2).
- o Clarifies procedures for access to IRR files (paras 3-2 and 3-3).
- o Adds sample certificates of understanding for signature of liaison DOD/non-DOD representatives (figs 3-1 and 3-2).
- o Includes an extract from sections 793 and 794, title 18, United States Code for required reading by the IRR representative (app B).
- o Includes an extract from section 9, Executive Order 10450, Security Requirements for Government Employment, 27 April 1953, Code of Federal Regulations for required reading by the IRR representative (app C).

Effective 25 September 1989

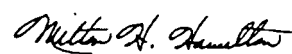
Military Intelligence

Investigative Records Repository

By Order of the Secretary of the Army:

CARL E. VUONO
General, United States Army
Chief of Staff

Official:



MILTON H. HAMILTON
Administrative Assistant to the
Secretary of the Army

History. This UPDATE printing publishes a revision of this publication. Because the publication has been extensively revised, the changed portions have not been highlighted.

Summary. This regulation establishes policies and procedures for storage, maintenance, transmission, review, and scheduled reduction of, as well as access to, investigative records in the custody of the Investigative

Records Repository (IRR). It outlines and clarifies requirements of the IRR, the U.S. Army Central Security Facility (CSF), the U. S. Army Intelligence and Security Command (INSCOM), and the Office of the Deputy Chief of Staff for Intelligence, Department of the Army (ODCSINT, DA) concerning these records.

Applicability. This regulation applies to the Active Army, Army National Guard (ARNG), and U.S. Army Reserve (USAR).

Internal control systems.

This regulation is subject to the requirements of AR 11-2. It contains internal control provisions, but does not contain checklists for conducting internal control reviews. These checklists are being developed and will be published at a later date.

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval of HQDA (DAMI-CIS), WASH DC 20310-1001.

Interim changes. Interim changes to this

regulation are not official unless they are authenticated by the Administrative Assistant to the Secretary of the Army. Users will destroy interim changes on their expiration dates unless sooner superseded or rescinded.

Suggested Improvements. The proponent agency of this regulation is the Office of the Deputy Chief of Staff for Intelligence, Department of the Army. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQDA (DAMI-CIS), WASH DC 20310-1001.

Distribution. Distribution of this publication is made in accordance with the requirements on DA Form 12-09-E, block number 3380, intended for command level B for Active Army, ARNG, and USAR.

Contents (Listed by paragraph and page number)

Chapter 1

General, page 1

Section I

Introduction, page 1

Purpose • 1-1, page 1

References • 1-2, page 1

Explanation of abbreviations and terms • 1-3, page 1

Section II

Responsibilities, page 1

IRR responsibilities • 1-4, page 1

Other responsibilities • 1-5, page 1

Chapter 2

Operating Procedures, page 1

Authorized files • 2-1, page 1

Accession criteria and procedures • 2-2, page 2

Transmission of materials • 2-3, page 2

File processing • 2-4, page 2

File storage and security • 2-5, page 3

Controlled dossiers • 2-6, page 3

File review • 2-7, page 4

File reduction and elimination • 2-8, page 4

Chapter 3

Access to IRR Dossiers, page 5

Dissemination of information about U.S. persons • 3-1, page 5

Procurement accounts • 3-2, page 5

File request procedures • 3-3, page 5

Accountability • 3-4, page 6

Return of IRR files • 3-5, page 6

Initial and supplemental materials • 3-6, page 6

Liaison accreditation • 3-7, page 7

Appendixes

A. *References, page 10*

B. *Extracts From Sections 793 and 794, Title 18, United States Code, page 11*

C. *Extract From Section 9 Executive Order 10450, Security Requirements for Government Employment, 27 April 1953, page 11*

Glossary

*This regulation supersedes AR 381-45, 10 August 1977.

RESERVED

Chapter 1 General

Section 1 Introduction

1-1. Purpose

This regulation outlines the responsibilities for operation of the Investigative Records Repository (IRR) and identifies the categories of materials authorized for IRR custody. It provides policies and procedures for the storage, maintenance, transmission, review, and systematic reduction of those records; establishes the appropriate uses to be made of IRR materials; and defines the procedures by which Department of Defense (DOD) and other official consumers may gain access to IRR holdings.

1-2. References

Required and related publications are listed in appendix A. Prescribed and referenced forms are also listed in appendix A.

1-3. Explanation of abbreviations and terms

Abbreviations and special terms used in this regulation are explained in the glossary.

Section II Responsibilities

1-4. IRR responsibilities

a. The Chief, IRR, is responsible for the operation of the Department of the Army (DA) records center, which serves as the repository for intelligence, counterintelligence (ci), security investigative and operational records (dossiers); related files that meet the criteria of this regulation; and required references created by or for the DA, and services requests by authorized consumers for information contained in those records.

b. Operational responsibilities include—

- (1) Receiving and entering the records into the center.
- (2) Researching and furnishing the files, extracts, or summaries to authorized requesters (includes files or responses related to National Agency Check (NAC) and litigation requests).
- (3) Reviewing dossiers for retention under the provisions of AR 25-400-2 and AR 381-10; downgrading of classified files under the provisions of AR 380-5; and ensuring that information contained in dossiers pertaining to U.S. citizens is complete, timely, accurate, and relevant in accordance with AR 340-21.
- (4) Ensuring that supplemental materials are promptly and accurately posted to SUBJECT dossiers.
- (5) Creating dossiers to accommodate new materials accessed in accordance with AR 381-10 and Deputy Chief of Staff for Intelligence (DCSINT) guidance.
- (6) Maintaining controlled files (para 2-6 below).
- (7) Updating IRR entries in the Defense Central Index of Investigations (DCII).
- (8) Coordinating with other headquarters and agencies to facilitate the processing of files and information.
- (9) Coordinating, accrediting, and monitoring the activities of all DOD liaison offices located within the IRR.
- (10) Monitoring and assisting liaison offices of non-DOD agencies accredited by DCSINT.

1-5. Other responsibilities

a. The Deputy Chief of Staff for Intelligence, Department of the Army (DCSINT, DA) will—

- (1) Define policy relating to the establishment and content of files in the IRR.
- (2) Establish access policies and restrictions upon dissemination of IRR materials within DA.
- (3) Take part in setting up agreements with other Government agencies for extended or permanent access to and use of IRR materials.

b. The Commander, U.S. Army intelligence and Security Command (CDR, INSCOM) will—

(1) Ensure the effective and efficient operation of the IRR through exercise of MACOM authority of U.S. Army Central Security Facility (USACSF).

(2) Provide or seek implementing guidance on DCSINT policy, as necessary.

c. The Commander, U.S. Army Central Security Facility (CDR, USACSF) will—

(1) Manage the IRR in compliance with applicable Federal statutes, this regulation, and the guidance of DCSINT and the Commander, INSCOM, in support of U.S. Army intelligence and ci activities.

(2) Accredite and monitor the DOD liaison offices within the IRR.

(3) Ensure timely response to requests from authorized consumers for investigative dossiers.

(4) Maintain a continuing files review program to identify and transfer or otherwise reduce files no longer authorized for IRR retention.

(5) Ensure appropriate segregation and security of controlled dossiers.

(6) Provide direction and control for the preparation of affidavits and supporting documents required by the Army General Counsel.

(7) Maintain disclosure accounting records in accordance with AR 340-21, paragraph 3-4.

Chapter 2 Operating Procedures

2-1. Authorized files

a. The following broad categories of materials are authorized for retention within the IRR. (See DA Pam 25-51, chap 6, for Privacy Act System notices referenced below.)

(1) *INSCOM investigative files.* Records relating to authorized intelligence or ci operations, missions, or investigations of persons, events, and organizations conducted by INSCOM (or predecessor DA agencies) or other DOD, Federal, State, or local investigative agencies. (Privacy Act System A0502.10aDAMI.)

(2) *Counterintelligence operations files.* Records obtained by or through agencies in subparagraph (1), above, in the conduct of foreign ci operations pertaining to counterespionage, counter-sabotage, countersubversion, and counterterrorism missions of the U.S. Army. (Privacy Act System A0503.06aDAMI.)

(3) *Technical surveillance index (TSI).* Records relating to persons whose conversations have been intercepted during technical surveillance operations conducted by, or on behalf of, the U.S. Army. (Privacy Act System A0502.03bDAMI.)

(4) *Intelligence collection files.* Records describing requirements, objectives, approvals, implementation, reports, and results of DA sensitive intelligence activities. (Privacy Act System A0502.03aDAMI.)

(5) *DA operational support activities files.* Documents concerning selected U.S. Army military members and civilian employees who have participated in U.S. Army intelligence and ci duties. (Privacy Act System A0503.03aDAMI.)

(6) *Personnel security clearance information files.* Documents relating to U.S. Army military and civilian employees and DA contractors on whom a personnel security clearance determination has been completed, is in process, or may be pending. (Privacy Act System A0506.01fDAMI.)

(7) *Other files.* Other ci, personnel security, and investigative files as directed by DCSINT.

b. IRR dossiers are both personal and impersonal in content and are classified for retention purposes under the following Modern Army Recordkeeping System (MARKS) categories (see AR 25-400-2, app B).

(1) Intelligence files (380-150 and 381- categories).

(2) Counterintelligence files (380-13 and 381-20 categories).

(3) Personnel security files (380 and 604 categories).

(4) Prisoner of War and civilian internee/detainee (PW/CI/D) files (608— category).

(5) Foreign liaison files (380—category).

c. The following types of materials will not be retained in the IRR:

(1) Personal or impersonal files of nonaffiliated U.S. SUBJECTS. (See AR 381–10, procedure 2, for exceptions to nonretention rule.)

(2) Files containing only materials originating from a non-DA agency.

(3) Impersonal files of a nonderogatory nature with last information more than 1 year old.

(4) Enemy PW/CI/D files in peacetime (except detailed debriefing statements of intelligence value).

(5) U.S. PW/CI/D files relating to individual U.S. prisoners (except detailed debriefing statements of intelligence value).

(6) Records of court-martial and nonjudicial punishment administered under article 15, Uniform Code of Military Justice, except as forwarded by the U.S. Army central clearance facility (CCF) as part of a personnel security adjudicative file.

d. Materials identified in paragraph c, above, may, however, be included in IRR files if those materials are exhibits or enclosures to an investigation or incident concerning a SUBJECT falling under purview of paragraph 2–1a above. Such materials will not be cross-referenced or otherwise identified in any investigative index.

2–2. Accession criteria and procedures

a. Material accessed into IRR dossiers, either initial or supplemental, will contain only one copy of each document having retention value for investigation, adjudication, security, or loyalty review, or containing information concerning persons or organizations of ci interest. All enclosures will be retained as part of the transmittal document to which they are attached, even if duplicated by an original copy or identical enclosure to another document elsewhere in the file. Original documents are preferred, but if this is not possible, the best available copy will be accessed. The following are examples of qualifying documents:

(1) DA Form 2784–R (Request for Counterintelligence Investigation), DD Form 1879 (Request for Personnel Security Investigation), or other similar documents initiating an investigation.

(2) Background documentation concerning the SUBJECT, to include DD Form 398 (DOD Personnel Security Questionnaire), Justice Form FD 258 (FBI U.S. Department of Justice Fingerprint Card (Applicant)), DD Form 398–2 (DOD Personnel Security Questionnaire National Agency Check), or other documents containing the results of examination of the records of agencies and digests of biographic information concerning a SUBJECT.

(3) Investigative reports with exhibits thereto.

(4) Defense Investigative Service (DIS) inquiries supporting limited investigations or adjudications.

(5) Key sheets referring to informants or technical processes. (See paras 2–2b and c below.)

(6) Case summaries prepared by control offices.

(7) Interrogatories, results of interrogations, interviews with the SUBJECT under oath, and statements executed by or on behalf of the SUBJECT.

(8) Correspondence or other documents pertaining to an investigation or adjudication.

(9) Extracts or summaries of reports of Inspector General (IG) investigations when they support a ci investigation. The authority directing an IG investigation will determine what information is to be included in the extract or summary. The dossier will not include the basic IG report of investigation. Requests for release of any portion of an IG report, including extracts or summaries therefrom, will be processed in accordance with the provisions of AR 20–1 (see para 3–4d(2) below).

(10) DA Form 2371 (Index Tracing Record of Aliases and Cosubjects).

(11) Correspondence relating to notification of denial or revocation of security clearance or access to sensitive compartmented information (SCI), DA Form 873 (Certificate of Clearance and/or

Security Determination), DA Form 3028–R (Limited Access Authorization), and reports submitted under provisions of AR 380–67 or AR 604–10.

(12) DA Form 5247–R (Request for Security Determination) and DA Form 5248–R (Report of Unfavorable Information for Security Determination) (and predecessor forms) with any enclosures or attachments thereto.

(13) DD Form 1300 (Report of Casualty).

(14) Polygraph examinations (see AR 195–6).

(15) Electronic surveillance material (formerly WIMEA) obtained in a manner consistent with applicable regulations and directives.

(16) Amendments to the record.

b. Confidential sources will be referenced in the dossier through use of a coded source key sheet. The IRR will maintain all key sheets in a sealed envelope with the SUBJECT's name and date of birth on the upper left corner, and the dossier number entered vertically on the right edge of the envelope.

c. Polygraph examination reports will be segregated from other dossier material, but maintained within the dossier of the individual to whom they pertain.

d. All material accessed must be certified retainable under AR 380–13 and AR 381–10 by the originator.

e. No investigative material will be filed in the IRR unless proper disposition is shown. A completed DD Form 1879 Request for Personnel Security Investigation must accompany the material.

2–3. Transmission of materials

a. All materials classified as TOP SECRET will be packaged and dispatched in accordance with the provisions of AR 380–5, chapter VIII.

b. All other materials, classified or not, will be afforded the same protection as SECRET information.

c. DA Form 3964 (Classified Document Accountability Record) or an inventory list of unclassified materials, as appropriate, will accompany each shipment. Both outer and inner envelopes will be addressed to the file procurement officer concerned (see para 3–2b below) and marked “TO BE OPENED BY ADDRESSEE ONLY.”

d. At a minimum, human intelligence (HUMINT) files will be transmitted with protections afforded SECRET material (see AR 381–100 (S)).

2–4. File processing

a. *Sources.* The IRR will accept initial or supplemental material from the following sources only:

(1) Case control offices with responsibility for ci activities for or on behalf of the U.S. Army.

(2) DA agencies authorized to conduct or support intelligence or ci operations.

(3) Agencies responsible for DA-level intelligence and ci products.

(4) U.S. Army Central Clearance Facility (CCF).

b. *Initiating and supplementing IRR dossiers.*

(1) All materials submitted for inclusion into the IRR as either initial or supplemental to an existing dossier will be evaluated under the criteria of this regulation (para 2–2 above) and AR 381–10 before accession. Only material related to any of the following descriptive categories will be accepted:

(a) Persons affiliated with the Department of Defense (see AR 380–13).

(b) Persons, organizations, and incidents of ci or security interest to the DA.

(c) Information concerning U.S. persons as authorized by AR 381–10.

(d) Alien persons or organizations that are the SUBJECT of authorized investigations.

(e) Alien persons or organizations identified in DA intelligence reports or other command intelligence reports.

(2) Materials requiring control custody, as defined in paragraph 2–6 below, or for which a control dossier already exists, will be processed by the IRR control custodian.

(3) Acceptable materials relating to a SUBJECT on which there

is no existing file will be accessed into the IRR as a new dossier; classified, as appropriate; assigned an identifying number; and entered in the DCII.

(4) Acceptable materials on which there is an existing SUBJECT dossier will be incorporated therein.

(a) The DCII will be adjusted to reflect the addition of the new material.

(b) The contents of the dossier will be purged of extraneous materials according to criteria defined in paragraph 2-7 below. Document and microfilm materials, if extant, will be consolidated before returning the file to storage.

(5) Cross-referencing will be accomplished only where doing so would serve legitimate intelligence, ci or security interests. Cross-referencing will not occur where doing so would cause a person or organization, otherwise of no legitimate interest, to appear in the DCII as the SUBJECT of a file.

(6) Exhibits will be handled as follows:

(a) The chain of custody for exhibits or items of evidence developed during an investigation, and which may be used in legal proceedings, extends to the IRR. Exhibits or items of evidence will be identified including the name of the SUBJECT, date and place of birth, social security number, and IRR dossier number, and will be appropriately identified with a cover sheet.

(b) Exhibits or evidence that are not required for routine investigations or adjudications normally will not be released to requesters.

(7) Initial or supplemental materials inappropriate for IRR retention will be returned to originating agency or office. Rejection of submitted materials will be based on the following criteria:

(a) *Substantive.* The material is outside the authority of this regulation or AR 381-10 for retention in IRR files.

(b) *Procedural.* The submission fails to meet the requirements defined in paragraph 3-6 below.

c. *Replies for requested files.*

(1) The IRR will expeditiously service requests from commanders and offices or agencies to which this regulation applies, and for which accreditation, as defined in paragraph 3-7, has been established. Circumstances or higher authority may require the processing of specific requests ahead of all others. Because of the disruption to IRR operations and the inevitable delays expedited processing inflicts on routine requests, expedited processing will be authorized under the most exceptional circumstances only by the Commander, USACSF.

(2) In the absence of a directed priority reply, the following order of precedence will be followed in processing requests for IRR files:

(a) Statutory action (for example, Freedom of Information Act and Privacy Act requests).

(b) Litigation actions to which the Army is a party.

(c) INSCOM investigations.

(d) Criminal investigations.

(e) Personnel security and security clearance actions.

(f) All others.

(3) Depending on the nature of the request, replies may be effected by sending the entire dossier or extracts or summaries thereof.

(a) Ordinarily, only the ODCSINT, the INSCOM Freedom of Information Act/Privacy Act office, INSCOM operational elements, and the U.S. Army central clearance facility may review an entire dossier. Case-by-case exceptions may be granted to other requesters by the Commander, USACSF, provided detailed justification is made.

(b) All accredited requesters other than subparagraph (a), above, will be provided, as appropriate, only a favorable response; a reproduced extract of unfavorable (derogatory) information; a summary of the requested dossier; or the response "nothing pertinent to your inquiry." Evaluation of unfavorable (derogatory) information for purposes other than file reduction or elimination, under the provisions of paragraph 2-8 below, is not an IRR responsibility.

(c) Non-DOD agencies will not be provided third-agency materials. The requester will be advised of the existence of such material and the identity of the agency having release authority.

(d) Financial records obtained on or after 10 March 1979 will not be disclosed outside DOD unless the requester certifies the relevance of such records in writing (see AR 190-6, para 2-8). A copy of the requesting justification and the release (or denial) authority will be permanently filed in the dossier concerned. Financial information obtained before 10 March 1979 may be released outside DOD according to existing records release procedures for ordinary records.

(e) The release of medical record information is governed by AR 40-66, AR 340-21, and AR 600-85. The written consent of the SUBJECT is required and will become part of the file before release. Signed releases will be forwarded to the Commander, USACSF, ATTN: IACSF-IR-E, Fort George G. Meade, MD 20755-5995.

d. *Accountability.*

(1) The IRR will develop and employ an inventory system that accounts for all files not in storage.

(2) Files will not ordinarily be loaned to any one requester for more than 60 calendar days. The IRR will develop a suspense system with appropriate followup notices to enforce the 60-day limit. Extensions based upon operational or other cogent justification may be granted by the Commander, USACSF.

e. *Concurrent interest.*

(1) Requests received while a file is on loan will be acknowledged with a reply indicating that the file in question is on loan to another agency and will provide resubmission instructions. The identity of the current or other waiting consumers, if any, will not be provided.

(2) The order of precedence established at paragraph c(2), above, will be observed in responding to multiple requests for the same file. The Commander, USACSF, may require the immediate return of a file to satisfy a priority request.

2-5. File storage and security

a. The information contained in IRR files, even the very existence of a file, constitutes a major trust placed in the U.S. Army by the source of that information. The existence of this bank of information, therefore, constitutes a significant potential liability if an unauthorized disclosure occurs. Consequently, all IRR files, regardless of classification or lack thereof, will be afforded at least the same protection as SECRET material. Controlled dossiers, as defined in paragraph 2-6, below, will be accorded the same protection as that for TOP SECRET material. Personnel assignments and access to and within the IRR will correspond to these circumstances (see AR 380-5, chap VII).

b. The volume of IRR materials and the nature of the IRR mission requires extraordinary measures to safeguard those materials and not overly encumber the service mission. The IRR facility, therefore, will be maintained in its entirety as a limited access area (see AR 190-13). Detailed security procedures recognizing the peculiar circumstances of the IRR will be locally developed, approved by the Commander, INSCOM, and rigorously enforced.

c. Investigative files within the IRR will be stored in such a way as to meet the following mission and security objectives:

(1) Efficient retrieval from and return to storage.

(2) Primary identification and storage by code number rather than SUBJECT name.

d. Dossiers shall be transmitted by any of the methods appropriate for SECRET and TOP SECRET materials as prescribed in AR 380-5, chapter VIII.

2-6. Controlled dossiers

Especially sensitive files will be maintained within the IRR in a limited access status, physically segregated from the main body of IRR materials.

a. The following two categories of controlled dossiers are authorized:

(1) *Category 1 (CD1).* Controlled dossiers that may be released to an authorized requester by the IRR control custodian only with the prior approval of the designating authority.

(2) *Category 2 (CD2).* Controlled dossiers that may be released

to an authorized requester by the IRR control custodian without prior approval of the designating authority.

b. The DCSINT, as control authority, shall establish policy and procedures for designating and releasing controlled dossiers.

c. Designating authorities shall—

(1) Request control of IRR dossiers on personnel under their jurisdiction, or in whom they have an official interest, that contain material warranting stringent control requirements.

(2) Designate the appropriate control category for each dossier identified (see paragraph *a* above).

(3) Review and certify the retainability of those dossiers and any new or supplemental material thereto in accordance with the criteria set forth in AR 381-10 and AR 340-21.

(4) Provide annual certification for continued retention in controlled status of all dossiers under their jurisdiction.

(5) Notify the IRR control custodian, in writing, when a dossier no longer needs to be controlled.

(6) Expeditiously respond to release coordination requests from the IRR control custodian.

d. The IRR control custodian will—

(1) Be responsible for the administrative processing, safeguarding, accountability, and custodianship of controlled dossiers (except those of selected INSCOM personnel, per paragraph 2-6*h* below).

(2) Approve or disapprove all requests for release of all controlled files.

(3) Access the dossiers of all officers selected or promoted to general officer or equivalent ranks into controlled status immediately upon notification of such selection or promotion.

(4) Coordinate with designating authorities when required in the exercise of their dossier control responsibilities.

e. Dossiers and supplemental materials thereto, relating to the following individuals or categories of content, will be accorded control status as follows:

(1) IRR military and civilian personnel and selected INSCOM personnel (CD1/CD2).

(2) Persons within the commands, agencies, or departments to which this regulation applies authorized to request dossiers from the IRR or having review or adjudicative functions in the personnel or industrial security program (CD2).

(3) Army officers (06 and below) and DA civilian employees assigned or detailed to another component of the U.S. intelligence community (CD1).

(4) All general and flag officers on active duty and for 1 year after retirement (CD2).

(5) General officer selectees (CD2).

(6) Secretaries of the Army and Defense (CD2).

(7) Individuals named or material identified by the controlling authority or a designating authority (CD1/CD2).

(8) Sources (potential, active, or dropped) and covert, clandestine, or confidential informants (CD1).

(9) Any person not otherwise specified in this paragraph who, by virtue of his or her assignment, might gain access to his or her own dossier (CD2).

(10) Persons listed as members of the family, or as relatives either in DD Form 398 or similar biographical information of persons listed in paragraphs 2-6*e* (1) through (9) above (CD2).

(11) Material that might reflect unfavorably upon foreign government officials (CD1).

(12) Electronic surveillance (ES) material (CD1). (This material will be segregated from the dossier and access will be controlled and recorded. A cross-reference sheet will be placed in the dossier to indicate that ES material has been removed and stored in a separate location.)

(13) Reports of IG investigations, extracts, or summaries thereof, when they support a ci investigation (CD1).

(14) All TOP SECRET and RESTRICTED DATA files (CD1).

f. Requests for control of individual dossiers may be made by designating authorities at any time by letter or electrical message to the Commander, USACSF, ATTN: IACSF-IR-A, Fort George G. Meade, MD 20755-5995. Each request will include the following:

(1) The category of control that is requested. Designating authorities specifying CD1 status for materials held in the IRR must be able to review or otherwise certify the releasability of that material to other authorized consumers within 10 days notice of such a request from the IRR control custodian.

(2) Reasons for request, as defined by paragraph 2-6*e*, above, with full justification whenever based on dossier content rather than the duty assignment or function of the individual.

(3) Duration of control, if known.

(4) Identification of personal data including date and place of birth, social security number, aliases, and IRR dossier number, if known.

g. Storage and transmission procedures are as follows:

(1) Controlled dossiers will be maintained in a distinguishable blue jacket and annotated as necessary with a precautionary warning. A permanent record of access for each dossier will be maintained at the controlled dossier storage area. The record will not accompany the dossier outside of the storage area.

(2) All dossiers in controlled status will be stored in an exclusion area within the IRR that meets the requirements of AR 380-5 for the storage of TOP SECRET material.

(3) Access to controlled dossiers will be limited only to personnel possessing both a TOP SECRET clearance and a requisite need to know. Requests for access will be processed in accordance with paragraph 2-4*c* above.

(4) Transmission of controlled dossiers shall be effected by any of the methods appropriate for TOP SECRET materials defined in AR 280-5. The inner envelope will be addressed to the receiving file procurement officer (see para 2-12*b* below) and marked "TO BE OPENED BY ADDRESSEE ONLY."

h. Dossiers of IRR personnel will be placed under control status by the INSCOM designating authority and maintained under physical custody of the Commander, INSCOM (IACSO), Arlington Hall Station, VA 22212-5000.

2-7. File review

a. Each dossier, document, or film on file in the IRR will be subjected to a systematic retention and security classification review each time it is retrieved from storage.

(1) Nonretainable files will be eliminated in accordance with paragraph 2-8 below.

(2) Retainable files will be purged of extraneous and duplicate materials and consolidated with existing film or document counterpart files, as appropriate.

(3) Classified files will be regraded or declassified under provisions of AR 380-5, chapters II and III.

b. The control custodian will ensure that all controlled dossiers are similarly reviewed while in and upon leaving controlled status.

2-8. File reduction and elimination

Every effort consistent with legitimate intelligence and security needs will be made to reduce the number and bulk of IRR files. Those objectives will be advanced by—

a. Elimination of duplication within retained dossiers.

b. Elimination of information within each file that is not complete, accurate, relevant, or timely in accordance with AR 340-21.

c. Eventual reduction of retained paper files to microform.

d. Elimination of nonretainable dossiers.

(1) Substantive retention criteria are established by this regulation and AR 381-10.

(2) Disposition instructions established by AR 25-400-2, paragraph 4-7, will apply.

e. File elimination will be accomplished under the provisions of AR 25-400-2, chapters 2 and 3.

(1) Overaged files of potential historical value will be offered to the National Archives and Records Administration (NARA) under procedures established by AR 25-400-2, paragraph 3 through 7, and AR 380-5, chapter III.

(2) Operational, technical, or confidential source material will not be transferred without approval of the Commander, INSCOM.

(3) Overaged files of no interest to NARA will be destroyed in

accordance with procedures for disposal of classified material established by AR 380-5.

(4) Appropriate entries will be made in all indices concerning transferred or destroyed dossiers.

Chapter 3
Access to IRR Dossiers

3-1. Dissemination of information about U.S. persons

The release of information concerning U.S. persons is governed by provisions of AR 340-21, paragraphs 3-1 and 3-2, and AR 381-10, procedure 4.

3-2. Procurement accounts

a. All agencies requiring access to IRR materials will establish a procurement account according to the following general guidelines. Each account will be assigned an identifying number by the IRR and be serviced through accredited file procurement officers (FPOs) (see para c below).

(1) Agencies and units requiring only occasional access to IRR files will utilize the account of a central office or higher headquarters to meet their needs.

(2) Ordinarily, procurement accounts will not be established below the division headquarters (military) or bureau (civilian) levels.

(3) The Pentagon Resident Office, 902d MI Group, will act as FPO for all accredited non-DOD agencies in the Washington metropolitan area.

(4) Exceptions may be made where geographic isolation, heavy volume, or other extraordinary circumstances warrant.

b. Correspondence relating to procurement accounts, including requests to establish an account, will be addressed to the Commander, USACSF (IACSF-IR-C), Fort George G. Meade, MD 20755-5995.

c. Concurrent with a request for a procurement account, correspondents will nominate at least two, but not more than four, individuals as FPOs. The FPO constitutes the sole point of contact between the accredited agency and the IRR for management of file requests and the receipt, control, and accountability of IRR files.

(1) FPO nominees must meet the following qualifications:

- (a) Have the minimum rank or grade.
 - 1. Military: Enlisted grade E-6, or commissioned or warrant officer.
 - 2. Civilian: Currently assigned to a position graded no lower than GS-5.
 - 3. Equivalent grade State or local official.

(b) Possess a valid SECRET clearance and be eligible for access to TOP SECRET information based on a minimum of a favorably completed background investigation.

(c) Be permanently assigned to the requesting organization.

(2) DD Form 577 (Signature Card) will be forwarded to the IRR for each nominee. The following information will be entered on the reverse side of each card:

- (a) Date and place of birth.
- (b) Social security number.
- (c) Security clearance status (degree of access, date of clearance, and authority).
- (d) Complete office telephone number (commercial, AUTOVON, FTS, and WATTS (where applicable)).

(3) FPOs of all accredited agencies will be thoroughly familiar with statutory and regulatory restrictions limiting the dissemination of ci information outside the receiving agency. This familiarization will include the following:

(a) The reading of extracts from the Espionage Laws (sections 793 and 794 title 18, United States Code), (app. B); and Executive Order 10450, 27 April 1953 (app C); AR 380-5; and AR 381-1 by each newly accredited representative.

(b) Instruction that disclosure of the contents, sources of information, or even the existence of an IRR dossier to persons not officially entitled to such information, may be made only when specifically authorized by the DCSINT; that material will not be added to or removed from any IRR dossier and the contents of an IRR dossier will not be altered, amended, or rearranged; and that IRR dossiers will be reviewed only in the course of official duties.

(4) A certificate of understanding (fig 3-1 or fig 3-2 as applicable to the nominating agency), prepared on agency letterhead, will be signed by each nominee and forwarded with agency FPO nominations for retention by the IRR.

d. Organizations with procurement accounts will, each January, submit a list of their accredited FPOs to the IRR. Delinquency will be cause for the IRR to terminate such accounts the following 1 April. Changes of FPO personnel will be reported as they occur to ensure continuity of access to IRR services. All correspondence relating to existing accounts will include the IRR-assigned account numbers and be addressed as shown in paragraph 3-2a above.

3-3. File request procedures

a. Requests for IRR materials in connection with intelligence, ci, security, or litigation matters will come through the accredited FPO to the Commander, USACSF (IACSF-IR-E), Fort George G. Meade, MD 20755-5995.

b. Requests usually will be made by mail on DA Form 1144 (Request for Dossier/Index Check). Full known identifying data will be provided for personal files, including full name (include all known maiden names or aliases), date and place of birth, social security number, and all pertinent cross-references. Impersonal files will be identified to the fullest extent possible by name, location, date of incident or event, and all pertinent cross-references. Dossier numbers will be included where known. The remarks section of the form will be used for nonstandard items of identification or to indicate the type of information, justification, or review desired, and whether it is a tracer or followup on a previous request. Non-DOD agencies will provide the appropriate code with their request (see table 3-1).

(1) Procurement accounts outside DA may use request forms developed by their own agencies for access to IRR materials, provided essential file-identifying data, as defined in paragraph 3-3b above, is supplied.

(2) Electrical message format may be used if expedited service is required. Justification will be provided in all cases. The Commander, USACSF, shall determine if priority processing is appropriate.

(3) Telephonic request will be accepted only under the most extraordinary circumstances; urgent requests should be made using an electrical message in accordance with paragraph 3-3b(2).

Table 3-1
Defense central index of investigations accounting codes for disclosures outside of DOD

Code: 01 Purpose: For use in current criminal law enforcement investigations, including statutory violations, counterintelligence, counterespionage, and other security matters. (Disclosure not releasable to SUBJECT without coordination with the agency to which record is disclosed.)
Code: 02 Purpose: To provide information for ongoing security and suitability investigations being conducted by non-DOD agencies for assignment of individuals to sensitive positions or for access. (Applicable to non-DOD agencies authorized to conduct full background investigations: OPM, FBI, IRS, USSS, BATF, Customs, DOS, Postal Service, and CIA.)
Code: 03 Purpose: To provide information pertinent to protection of persons under the provisions of 18 USC 3056. (Disclosure not releasable to the SUBJECT without approval of USSS.)
Code: 04 Purpose: To provide information in judicial or adjudicative proceedings, including litigation, or in accordance with a court or congressional inquiry.

Table 3-1
Defense central index of investigations accounting codes for disclosures outside of DOD—Continued

Code: 12

Purpose: To Federal agencies to confirm the investigation or clearance of individuals.

Code: 13

Purpose: To the Comptroller General, or any authorized representative, in the course of the performance of the duties of the General Accounting Office.

Code: 14

Purpose: To a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual.

Code: 15

Purpose: To the National Archives and Records Administration (NARA) as a record that has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the NARA to determine whether or not the record has such value.

3-4. Accountability

a. Each account holder is responsible for safeguarding IRR dossiers during the time they are in his or her possession, or until relieved of responsibility by a returned receipt from the IRR. Direct transfer of dossiers to another account holder is prohibited.

b. Each dossier will be afforded the protection appropriate to its classification, but in no case less than that prescribed for SECRET material by AR 380-5.

(1) Only persons with an appropriate security clearance and a legitimate need to know will be permitted access to IRR materials. In no case will the SUBJECT of a dossier be allowed access to his or her own file.

(2) Unauthorized disclosure of the contents of a dossier constitutes a compromise of privileged, often classified information. The provisions of AR 340-17 and AR 380-5, chapter VI, apply. Additionally, the accountable FPO will immediately advise the Commander, USACSF, of all particulars concerning the compromise.

(3) In the event of a missing or lost dossier, the accountable FPO will—

(a) Provide the Commander, USACSF, by the most expeditious means available, all known details concerning the loss, including the name of the person responsible for security of the dossier at the time of the loss.

(b) Make an immediate and continuing search for the missing document(s).

(c) Inform the appropriate commander that an investigation under the provisions of AR 15-6 or AR 380-5 into the circumstances surrounding the loss is required. (A copy of the report of investigation and a report of final command action taken will be forwarded to the Commander, USACSF.)

c. Personnel having temporary custody of permanent copies of IRR records are prohibited from removing any material from dossiers, except—

(1) When specifically directed or authorized by the DCSINT. In such cases, the request for removal of material, including the justification or reason and the approval or direction of the DCSINT, together with the final action, will become a permanent part of the dossier. Actual removal of material will be accomplished by IRR personnel.

(2) When necessary for reproduction. Material removed will be replaced in the dossier immediately after reproduction in the same location from which removed.

d. Except where otherwise authorized by current regulations (ARs 340-17, 340-21, 380-5, 381-1, 381-20, or 604-10) or directives, documents may be copied, extracted, or reproduced from dossiers only to meet investigative, adjudicative, administrative,

court martial, administrative board action, and assignment requirements. Commanders of major Army commands and commanders of their major subordinate elements may release information from ci investigative reports to duly constituted boards and courts convened to try individuals for activities revealed by such investigations. The identity of confidential sources or other Federal Government agencies providing information will not be disclosed without the prior written consent of the Commander, INSCOM, or higher authority.

(1) Classified material may be reproduced only in accordance with provisions of AR 380-5, paragraph 7-305.

(2) Copying, extracting, reproducing, or releasing information from IG reports is subject to the provisions of AR 20-1. Ordinarily, IG materials constituting a portion of a dossier will not be provided in response to requests. Case-by-case justification must be made through the Commander, USACSF, for final determination by The Inspector General in accordance with AR 20-1.

(3) Financial records will be disseminated to non-DOD agencies only in accordance with paragraph 2-4c(3)(d) above.

(4) Medical records will be disseminated to non-DOD agencies only in accordance with paragraph 2-4c(3)(e) above.

(5) Copies, extracts, or reproductions made for DOD agencies will be marked or stamped as follows: "INFORMATION COPY (EXTRACT) ONLY. TO BE DESTROYED UPON COMPLETION OF ACTION. RECORD COPY ON FILE AT IRR, USACSF, FORT GEORGE G. MEADE, MD 20755-5995."

(6) Copies, extracts, or reproductions for agencies outside the DOD will contain no third-agency material and will be marked or stamped as follows: "THIS IS A COPY (EXTRACT) OF AN INVESTIGATIVE RECORDS REPOSITORY, USACSF, FORT GEORGE G. MEADE, MD 20755-5995. IT IS FURNISHED WITHOUT PRIOR PERMISSION OF THE COMMANDER, USAINSCOM, OR DCSINT. IT DOES NOT CONSTITUTE A DEPARTMENT OF THE ARMY DETERMINATION REGARDING THE SUBJECT."

(7) FPOs are responsible for ensuring that materials are appropriately safeguarded from unauthorized disclosure and destroyed promptly following completion of the purpose for which they are produced.

e. Except as provided in paragraph 3-4c above, only the IRR may modify the contents of a dossier by adding or removing material. Supplemental materials will be submitted in accordance with paragraph 3-6 below. Material may be submitted concurrent with the return of a dossier, provided that the material is identified as new and attached to the outside of the basic file.

3-5. Return of IRR files

a. Dossiers are to be returned to the IRR as soon as possible after the need for them has been met. Ordinarily, this should be within 60 calendar days of their dispatch from the IRR (see para 2-4d above).

b. Dossiers will be dispatched in the same manner and afforded the same protection as when sent from the IRR (see para's 2-3 and 2-6f above).

c. The inventory card that accompanied the dossier from the IRR, or a completed DA Form 3964, as appropriate, will be included with all returned materials.

3-6. Initial and supplemental materials

a. Criteria and procedures for submission of materials are defined in paragraphs 2-1 and 2-2 above.

b. Materials for inclusion in the IRR will be forwarded to the Commander, USACSF (IACSF-IR-E), Fort George G. Meade, MD 20755-5995. Identifying data, as required by paragraph 3-3 above, will be included with the submission.

c. Initial and supplemental material forwarded to IRR will not contain convenience copies of investigative reports and correspondence, documents of a general administrative nature pertaining to personnel or logistical management, rough draft notes, or documents for which another DA agency is the primary office of record, unless such documents directly pertain to a ci or security investigation or to a security or loyalty adjudication.

d. Agencies other than those identified in paragraph 2-4a, above,

wishing to include material into the IRR will route such material through one of the authorized source agencies.

3-7. Liaison accreditation

a. DOD accreditation

(1) Major Army commands and other DOD agencies may submit requests to accredit liaison representatives directly to the IRR. Spaces and funding must come from the requester. If full-time liaison representation is not warranted, major commands may designate representatives to visit the IRR as required. Each liaison representative must be accredited by the Commander, USACSF, before being sent to the IRR (see para 3-2b(1) above).

(2) All DOD agencies seeking IRR liaison representation must possess a valid requirement for the information by virtue of mission and need to know.

(3) Requests for accreditation to the IRR will be submitted to the Commander, USACSF (IACSF-IR-C), Fort George G. Meade, MD 20755-5995, and will include the following:

(a) The name and full address of the office, agency, or command seeking accreditation.

(b) Full identifying data on the liaison agent nominee(s) (see para 3-2b(2) above).

(c) A statement of justification outlining requirements for access to IRR records.

b. Agencies other than DOD.

(1) Non-DOD agencies seeking liaison access to the IRR must be accredited by DCSINT. Requests for accreditation will be submitted to HQDA (DAMI-CIS), WASH DC 20310-1001, and will conform to the specifications in paragraph 3-7a(3) above.

(2) Liaison representatives of accredited non-DOD agencies will receive the same indoctrination required of FPOs (see para 3-2b(3) above), and execute the appropriate certificate of understanding (fig 3-1 or fig 3-2).

(3) Operational and third-agency rule limitations are as follows:

(a) Dossiers requested by agencies or their liaison representatives will be screened by IRR personnel before release.

(b) Materials divulging operational methods or identifying confidential or coded sources will not be disclosed without prior approval of the DCSINT.

(c) Materials supplied by other than DOD components as well as the agency that provided such information will not be disclosed. However, the existence, identity, and source of such information will be provided.

SAMPLE CERTIFICATE OF UNDERSTANDING
BY REPRESENTATIVES OF AGENCIES SIGNATORY TO THE
DELIMITATIONS AGREEMENT (DOD Agencies and FBI)

AGENCY LETTERHEAD

DATE 15 June 1989

1. As an accredited representative to the Investigative Records Repository (IRR), I have access to counterintelligence investigative dossiers of the U.S. Army.

2. The agency that I represent is a signatory to the Delimitations Agreement. As its accredited representative, I understand that in the performance of my official duties at the IRR:

a. I may copy, quote, summarize, and otherwise disseminate to my agency information from U.S. Army sources.

b. I may summarize or copy information in IRR records originated by other signatory agencies provided that the material does not contain any restrictions by the originating agency.

c. I may not extract, quote, summarize, or otherwise disseminate information in IRR dossiers originated by U.S. agencies that are not signatory to the Delimitations Agreement. With respect to such data, I may note the title, date, and originating office of such information.

d. I may not alter, amend, or rearrange material contained in an IRR dossier, nor may I add or remove material.

3. I have read, understand, and will comply with the restrictions concerning the dissemination of classified defense and Privacy Act information set forth in AR 380-5 (Department of the Army Supplement to DOD 5200.1-R (DODISPR)) and AR 340-17 (Release of Information and Records from Army Files). I will not circulate U.S. Army counterintelligence information, which I may receive in the conduct of my duties, outside my agency without the consent of the IRR.


(Signature)

JOHN B. SMITH

(Typed Name)

ODCSINT. HQDA (DAMI-CI)

Washington, DC 20310-1001

(Agency/Agency Address)

Figure 3-1. Sample Certificate of Understanding (DOD or FBI)

SAMPLE CERTIFICATE OF UNDERSTANDING BY REPRESENTATIVES
OF AGENCIES NOT SIGNATORY TO THE DELIMITATIONS AGREEMENT
(Other Than DOD Agencies or FBI)

AGENCY LETTERHEAD

DATE 15 June 1989

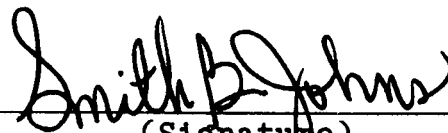
1. As an accredited representative to the Investigative Records Repository (IRR), I have access to counterintelligence dossiers of the U.S. Army.

2. The agency that I represent is not a signatory to the Delimitations Agreement. As its accredited representative, I understand that in the performance of my official duties at the IRR:

a. I may copy, quote, summarize, or otherwise disseminate to my agency, only information obtained from U.S. Army sources.

b. I may not alter, amend, or rearrange material contained in an IRR dossier, nor may I add or remove material.

3. I have read, understand, and will comply with the restrictions concerning the dissemination of classified defense and Privacy Act information as set forth in AR 380-5 (Department of the Army Supplement to DOD 5200.1-R (DODISPER)), and AR 340-17 (Release of Information and Records from Army Files). I will not circulate U.S. Army counterintelligence information, which I may receive in the conduct of my duties, outside my agency without consent of the IRR.


(Signature)

SMITH B. JOHNS
(Typed Name)

OPM. Ofc of Fed Investigations

USOPM-OFI. Wash DC 20044
(Agency/Agency Address)

Figure 3-2. Sample Certificate of Understanding (Non-DOD or FBI)

Appendix A References

Section I Required Publications

AR 25-400-2

The Modern Army Recordkeeping System (MARKS). (Cited in paras 1-4b(3)(a), 2-1b, 2-8c(1) and (2), and 2-8d and 2-8d(1).)

AR 40-66

Medical Record and Quality Assurance Administration. (Cited in para 2-4c(3)(e).)

AR 190-6

Obtaining information from Financial Institutions. (Cited in para 2-4c(3)(d).)

AR 340-17

Release of Information and Records from Army Files. (Cited in para 3-4b(2) and 3-4d.)

AR 340-21

The Army Privacy Program (Cited in para 3-4d.)

AR 380-5

Department of the Army Information Security Program. (Cited in paras 1-4b(3)(b), 2-1b(3), 2-3a, 2-5a, 2-5d, 2-6f(2) and (4), 2-7a (3), 2-8d(1) and (3), 3-2b(3)(a), 3-4b, b(2) and b(3)(c) , and 3-4d and d(1).)

AR 380-10

Department of the Army Policy for Disclosure of Information, Visits, and Accreditation of Foreign Nationals. (Cited in paras 1-4b(3)(a), 1-4b(5), and 3-1.)

AR 380-13

Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations. (Cited in paras 2-2d and 2-4b(1)(a).)

AR 380-67

Personnel Security Program. (Cited in paras 2-1b(3) and 2-2a(11).)

AR 381-10

U.S. Army Intelligence Activities. (Cited in paras 1-4b(3)(a), 1-4b(5), 2-1c(1), 2-2d, 2-4b(1), 2-4b(7)(a), 2-6b(3), 2-8c(1), and 3-1a.)

AR 381-20

U.S. Army Counterintelligence Activity. (Cited in para 2-1b(2).)

AR 604-10

Military Personnel Security Program. (Cited in paras 2-2a(11) and 3-4d.)

DA Pam 25-51

The Army Privacy Program—System Notices and Exemption Rules. (Cited in paras 2-1b(1) through 2-1b(4).)

Section II Related Publications

A related publication is merely a source of additional information. The user does not have to read it to understand this regulation.

AR 11-2

Internal Control Systems

AR 15-6

Procedures for Investigating Officers and Boards of Officers

AR 20-1

Inspector General Activities and Procedures

AR 190-13

The Army Physical Security Program

AR 195-6

Department of the Army Polygraph Activities

AR 380-150

Access to and Dissemination of Restricted Data

AR 381-1

Control of Dissemination of Intelligence Information

AR 381-100 (S)

Army Human Intelligence Collection Programs (U)

AR 600-85

Alcohol and Drug Abuse Prevention Program

Section III Referenced Forms

DA Form 1144

Request for Dossier/Index Check (Prescribed in para 3-3b)

DA Form 2371

Index Tracing Record of Aliases and Cosubjects

Section IV Referenced Forms

DD Form 398

DOD Personnel Security Questionnaire

DD Form 398-2

DOD Personnel Security Questionnaire National Agency Check Request

DD Form 577

Signature Card

DD Form 1300

Report of Casualty

DD Form 1879

Request for Personnel Security Investigation

DA Form 12-9

Subscription for DA Unclassified Administrative Publications

DA Form 873

Certificate of Clearance and/or Security Determination

DA Form 2028

Recommended Changes to Publications and Blank Forms

DA Form 2784-R

Request for Counterintelligence Investigation

DA Form 3028-R

Limited Access Authorization

DA Form 3964

Classified Document Accountability Record

DA Form 5247-R

Request for Security Determination

DA Form 5248-R

Report of Unfavorable Information for Security Determination

Appendix B
Extracts From Sections 793 and 794, Title 18, United States Code

Section 793. Gathering, transmitting, or losing defense information.

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any document, writing, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or “(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, note or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of his trust or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer—Shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.”

Section 794. Gathering or delivering defense information to aid foreign government

“(a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life.”

Appendix C
Extract From Section 9 Executive Order 10450,
Security Requirements for Government
Employment, 27 April 1953

Section 9.

“(c). The reports and other investigative material and information developed by investigations conducted pursuant to any statute, order, or program described in section 7 of this order shall remain the property of the investigative agencies conducting the investigations, but may, subject to considerations of the national security, be retained by the department or agency concerned. Such reports and other investigative material and information shall be maintained in confidence, and no access shall be given thereto, except with the consent of the investigative agency concerned, to other departments and agencies conducting security programs under the authority granted by or in accordance with the said act of Aug 26, 1950, as may be required for the efficient conduct of Government business.”

Glossary

Section I Abbreviations

ARNG

Army National Guard

BATF

Bureau of Alcohol, Tobacco and Firearms

CCF

central clearance facility

CD

controlled dossier

ci

counterintelligence

CIA

Central Intelligence Agency

CSF

Central Security Facility

DA

Department of the Army

DCII

Defense Central Index of Investigations

DCSINT

Deputy Chief of Staff for Intelligence

DIS

Defense Investigative Service

DOD

Department of Defense

DOS

Department of State

ES

electronic surveillance

FBI

Federal Bureau of Investigation

FPO

file procurement officer

HQDA

Headquarters, Department of the Army

HUMINT

human intelligence (the intelligence collection function that uses human beings as both sources and collectors)

IG

Inspector General

INSCOM

U.S. Army Intelligence and Security Command

IRR

Investigative Records Repository

IRS

Internal Revenue Service

MARKS

Modern Army Recordskeeping System

NAC

National Agency Check

NARA

National Archives and Records Administration

ODCSINT, DA

Office of the Deputy Chief of Staff for Intelligence, Department of the Army

OPM

Office of Personnel Management

PW/CI/D

prisoner of war/civilian internee/detainee

SCI

sensitive compartmented information

TSI

Technical Surveillance Index

USACSF

U.S. Army Central Security Facility

USAR

U.S. Army Reserve

USSS

U.S. Secret Service

Section II Terms

Control office

The agency or organization exercising directive authority over an investigation or collection activity.

Controlled dossier

Files of a particularly sensitive nature due to substantive content or method of collection, which are physically segregated from the body of ordinary materials.

Cross-reference

The identification of the SUBJECT of one dossier with the SUBJECT of another by virtue of an alias or some association or activity of legitimate intelligence or ci significance.

Customer

A Government agency that requires IRR information either to produce other intelligence or for decision-making purposes. Synonymous with "user," "requester," and "consumer."

Defense Central Index of Investigations

The automated alpha-numeric register of DOD investigations; maintained by the DIS.

Delimitation Agreement

Agreement between the Deputy Secretary of Defense and the Attorney General of the

United States that establishes delimitation of responsibilities for ci investigations.

Designating authority

The commander or senior official of a unit, agency, or office having the responsibility for identifying specific IRR dossiers for controlled status and the degree of control.

DOD agency

Any department, office, bureau, or organization subject to the authority of the Secretary of Defense. Synonymous with "DOD component."

Dossier

An official file of investigative, intelligence, or ci materials collected by or on behalf of the U.S. Army. May consist of documents, film, magnetic tape, photographs, or a combination thereof. Synonymous in this publication with "file" or "record." May be "personal" referring to an individual, or "impersonal" referring to a thing, event, or organization.

Initial material

Information on a SUBJECT for which there is no known existing dossier.

Liaison representative

An official representative of an agency accredited to request and review dossiers onsite at the IRR, Fort George G. Meade, MD. Synonymous herein with "liaison office."

Litigation

Any legal proceeding to which the U.S. Government, DOD, its component departments or agencies, or any individual thereof in an official representative capacity is a party.

Retention

The maintenance of information that can be retrieved by reference to name or other identifying data (e.g., dossier number). (Information on U.S. persons that is authorized for retention is defined in AR 380-10. The length of retention period is specified in AR 25-400-2.)

a. Limited retention. Material that may be stored for up to 75 years beyond the date of last information. Such material will be destroyed following the end of the prescribed holding period.

b. Permanent retention. Material to be preserved indefinitely by NARA following the end of authorized limited retention by DA.

SUBJECT

The person, organization, event, or thing to which a dossier pertains.

Supplemental material

New information on a SUBJECT for which a dossier already exists. Synonymous with "additional material."

Third-agency rule

The governing rule that states that, except as provided in section 102, National Security

Act of 1947, classified information originating in one U.S. agency (e.g., DOD) will not be disseminated by another agency to which the information has been made available without the consent of the originating agency.

U.S. Intelligence community

The collective intelligence apparatus of the United States, composed of—

- a.* The Central Intelligence Agency (CIA).
- b.* The National Security Agency (NSA).
- c.* The Defense Intelligence Agency (DIA).
- d.* DOD components for the collection of national foreign intelligence, via reconnaissance programs.
- e.* The Bureau of intelligence and Research, U.S. Department of State.
- f.* The intelligence elements of the military services of the United States.
- g.* The Federal Bureau of Investigation (FBI).
- h.* The U.S. Department of the Treasury.
- i.* The U.S. Department of Energy.
- j.* The staff elements of the Director of Central Intelligence.

U.S. person

A U.S. citizen, permanent U.S. resident alien, any organization substantially composed of U.S. citizens or permanent U.S. resident aliens, or any organization incorporated under the laws of a State or the United States, but not directed by a foreign government or governments. Synonymous with U.S. SUBJECTS. (See AR 381–10, app A, para 27.) There are no special terms.

USAPA

ELECTRONIC PUBLISHING SYSTEM
TEXT FORMATTER ... Version 2.45

PIN: 004117-000

DATE: 10-19-98

TIME: 15:12:01

PAGES SET: 17

DATA FILE: ar381-45.fil

DOCUMENT: AR 381-45

DOC STATUS: NEW PUBLICATION